REMARKS

Claims 1-6, 8-12, and 14-23 are pending. Claims 1, 4, 10-11 and 15 are amended, and new claim 23 is added with this response. Reconsideration of the application is respectfully requested based on the following remarks.

I. REJECTION OF CLAIMS 1-6, 8-12, and 14-22 UNDER 35 U.S.C. § 102(e)

Claims 1-6, 8-12, and 14-22 were rejected under 35 U.S.C. § 102(e), as being anticipated by U.S. Patent No. US 6,963,946 B1 Dwork et al. (Dwork). Withdrawal of the rejection is respectfully requested for at least the following reasons.

Independent claim 1 has been amended to recite a network interface system comprising *a descriptor management system adapted to obtain initialization vector information from the host system and to provide the initialization vector information to the security system.* Additionally, ***the security system is adapted to employ an initial random data string from the outgoing data to begin encryption before security association information has been retrieved by the security system.***

Although network controller 102 of Dwork also comprises a security system 124 (See, *e.g.*, Figs. 2 and 3), the security system of Dwork is not ***adapted to employ an initial random data string from the outgoing data*** (See, *e.g.*, initialization vector 226 of Fig. 1F, and outgoing data frame 200 of Fig. 1E and 1F) ***to begin encryption before security association information has been retrieved by the security system.*** (See, *e.g.*, Applicants' specification page 16, lines 10-16, 24-28).

By contrast, Dwork teaches using **Security Association (SA)** information for obtaining such information for encryption (reference Dwork, column 14, lines 45-54), and therefore must wait until this SA information has been retrieved by the security system before the encryption recited in claims 1 and 15 can begin. For example, the DMU 130 of the network interface system 102 described by Dwork describes utilizing Security Associations (SAs) from an SA memory 140 which are obtained prior to security processing. Therefore Dwork et al. fail to anticipate the invention of claim 1.

and the claims which depend therefrom. Accordingly, withdrawal of the rejection is respectfully requested.

In addition, Claims 10 and 11, for example, further recite that the security system selectively employs an initialization vector (IV) (*e.g.*, 226 of Fig. 1F) comprising the initial random data string from the outgoing data to perform CBC encryption according to the initialization vector information, wherein the security system is adapted to use the initial random data string as **a seed value for encrypting the first block of cyphertext before the security association information has been retrieved by the security system.** (See, *e.g.*, Applicants' specification page 16, lines 12-13, 24-28).

Further, although the descriptor management system 130 of Dwork also comprises initialization vector length bits IVLEN0 and IVLEN1 in the TFLAGS1 byte 193 of transmit descriptor 192a (*e.g.*, col. 24, ll. 54-59, and Figs. 5E and 5F), such length bits of Dwork are not "inherently" initialization vectors (*e.g.*, IV 226) comprising a random data string that can be used by the security system to facilitate high-speed data encryption **before security association information has been retrieved by the security system.**

In one non-limiting example, the inventors have appreciated that in network interface systems, such as the systems 2 and 102 described in the present invention, in which security processing is performed outside the host system 6, that the security processing system 124 must be able to differentiate between outgoing data frames 200 that include an IV 226 (*e.g.*, as illustrated in Fig. 1F) and those that do not (Fig. 1E). In the example systems of the present invention, initialization vector information 191 is provided to the security processing system 124 by the descriptor management system 130, to indicate whether an IV 226 is present in the frame 200, and if so, the length of the IV 226. Although such information may be derived from the security association (SA) associated with a particular data frame 200, the provision of the information 191 by the descriptor system 130 advantageously allows the encryption to begin before the SA information has been retrieved by the security processor 174, thus facilitating high-speed data encryption to meet gigabit wire speeds.

Therefore Dwork et al. fail to anticipate the invention of claim 1 and the claims which depend therefrom. Accordingly, withdrawal of the rejection is respectfully requested.

Similarly, independent claim 15 has been amended to be directed to *a method of encrypting outgoing data in a network interface system, comprising* ***selectively encrypting outgoing data according to an initialization vector (IV) comprising an initial random data string*** *from the outgoing data,* ***before security association information has been retrieved by the security system.***

By contrast, Dwork does not discuss ***selectively encrypting outgoing data according to an initialization vector (IV) comprising an initial random data string.*** Further, Dwork does not discuss encrypting ***before security association information has been retrieved by the security system,*** because Dwork teaches encryption based on the use of **security associations** after they are retrieved by the security system.

Therefore the cited art does not anticipate the claimed invention of independent claims 1 and 15, and the claims which depend therefrom. Accordingly, withdrawal of the rejection is respectfully requested.

II. CONCLUSION

For at least the above reasons, the claims currently under consideration are believed to be in condition for allowance.

Should the Examiner feel that a telephone interview would be helpful to facilitate favorable prosecution of the above-identified application, the Examiner is invited to contact the undersigned at the telephone number provided below.

Should any fees be due as a result of the filing of this response, the Commissioner is hereby authorized to charge the Deposit Account Number 50-1733, AMDP763US.

Respectfully submitted,
ESCHWEILER & ASSOCIATES, LLC

By /Thomas G. Eschweiler/
Thomas G. Eschweiler
Reg. No. 36,981

National City Bank Building
629 Euclid Avenue, Suite 1000
Cleveland, Ohio 44114
(216) 502-0600